

Sécurisez vos réseaux Internet et Intranet
Protégez-vous des attaques et garantisiez la fiabilité de vos données

Plan de la formation

Introduction

- Objectif du stage
- De l'informatique... aux Systèmes d'Information
- L'ouverture des Systèmes d'Information des entreprises et des organisations
- Les risques liés à l'ouverture : mythe ou réalité ?
- Quelle est votre responsabilité ?

I. La sécurité des réseaux

1. Les besoins d'exploitation à satisfaire

- Accéder à Internet depuis le réseau intérieur
- Echanger des messages
- Fournir un site Intranet, un site Extranet, un site Internet (web)

2. Les objectifs de sécurité à atteindre

- Que doit-on sécuriser/protéger et pourquoi ?
- Les données
- Les ressources
- La réputation

3. La démarche sécurité

- Le cycle Réflexion > Action > Contrôle
- La Politique de Sécurité Informatique et Informationnelle (P.S.I.I.)
- Un exemple de P.S.I.I. en 10 étapes
- Les rôles respectifs des différents acteurs de la sécurité
- Le système de sécurité doit évoluer parallèlement au Système d'Information

II. La mise-en-œuvre de la sécurité réseau

1. Les pré-requis

- La bonne connaissance du Système d'Information et de son infrastructure
- Une bonne architecture réseau (simplicité et clarté)

2. Connecter son réseau à Internet

- Connecter son réseau intérieur sur le(s) réseau(x) extérieur(s)
- Réseau intérieur / Serveur http, ftp, smtp... / Réseau extérieur / Client extérieur
- Le protocole TCP/IP
- Se connecter au réseau intérieur depuis le réseau extérieur
- Les différents types d'accès, la gestion des accès

Atelier n°1 : 2° jour

« Clients et serveurs HTTP »

3. L'objectif de cloisonnement des réseaux

- Le cloisonnement des réseaux
- Le Firewall est un poste de contrôle

4. Proxy et Firewall : les outils du cloisonnement

- Le « Proxy »
- Le plan d'adressage IP du réseau intérieur (RFC 1918)
- La place du Firewall dans le système de sécurité
- Les fonctions du Firewall : 1) La translation d'adresses, 2) Le filtrage des paquets, 3) Les relais applicatifs
- Les fonctions complémentaires au filtrage
- Les différentes architectures du Firewall et son intégration au SI
- Les réseaux « sas » ou DMZ

5. L'administration du Firewall

- a) Mise en place :
 - Installation du Firewall sur le bastion
 - Définition et paramétrage des règles de sécurité
- b) Mise en œuvre :
 - Tests et administration
 - Analyse du trafic et des incidents
 - Réponses aux incidents et aux attaques

Atelier n°2 : 3° jour

« FireWall-1 de Check Point »

III Les risques / les fonctions de sécurité à assurer / les outils de sécurité

1. Les risques encourus

- Les menaces potentielles / La sensibilité de l'entreprise ou de l'organisation
- Les menaces avérées / L'exposition du système d'information
- Les incidents / La vulnérabilité du système d'information
- Les attaques : deni de service, virus, intrusion... / La vulnérabilité du système d'information
- Les dégâts / La dommageabilité du système d'information
- Les conséquences pour l'entreprise / La capacité de récupération (réparation et compensation)

2. Les fonctions de sécurité à assurer

- Niveau de sécurité souhaité, contraintes et mise-en-œuvre
- Authentification (PAP, CHAP)
- Contrôle d'accès
- Confidentialité
- Intégrité
- Non répudiation

3. Sécuriser et protéger

- Définition des moyens de détecter, de déjouer ou de neutraliser et d'atténuer les attaques : les moyens de protection à mettre en place

- Les outils de sécurité existants
- La sécurité « client » : le poste client, les options de sécurité des navigateurs
- La sécurité « serveur » : le poste serveur, l'administration du serveur
- La sécurité « Internet » : les attaques sur Internet

4. La cryptographie

- Les bases de la cryptographie
- La cryptographie asymétrique et la Public Key Infrastructure (P.K.I.)
- Les certificats et leur gestion
- Les Réseaux Privés Virtuels (RPV, VPN)
- La législation

Atelier n°3 : 4° jour

« Attaques et Parades »

Prise de contrôle à distance (cheval de Troie), écoute de ligne et parade d'authentification, chiffrement des données...

Conclusion

- Pas de sécurité sans simplicité et clarté.
- Pas de sécurité sans démarche et méthode.
- Pas de sécurité sans suivi et évolution du système de sécurité.
- La nouvelle approche de la sécurité informatique doit être globale.
- Pas de sécurité sans l'implication de Tous.